REMARKS

Applicant thanks the Examiner for withdrawing the previous rejection.

Prior Art Rejections

Claims 1, 2, 4-9, 11-19, and 24-30 stand rejected under 35 U.S.C. § 103 as being unpatentable over Nakagawa (U.S. Pub. 2001/0028725) in view of Van Rijnsoever (U.S. Pub. 2002/0090090).

Claims 3 and 10 stand rejected under 35 U.S.C. § 103 as being unpatentable over Nakagawa in view of Van Rijnsoever and further in view of Clark et al. (U.S. Pat. 5,864,747).

Applicant respectfully traverses the rejections.

Neither Nakagawa nor Van Rijnsoever, taken alone or in combination, disclose or suggest all of the claimed limitations. Nakagawa merely discloses a data protection technique which appears to rely on scrambling of encoded data. See, Abs., fig. 1. Nakagawa does not appear to use encryption, as recited by Applicant's claims. While the Examiner kindly points to ¶ 19 which uses the word "encryption", such use is clearly discussing encoding/decoding, rather than encryption. This reference, which may well be a misprint or translation error, appears be the only use of the term encryption in the voluminous and detailed disclosure of Nakagawa. The bulk of the disclosure clearly discusses encoding, specifically naming MPEG – 4 encoding. Those of skill in the art will readily appreciate that, encryption generally restricts access to distributed content, and does not generally aid in the insertion of watermarks nor prevent a user which has access to the content from making unauthorized copies of the content, as suggested in ¶ 19, such later function is generally performed by a user device's adherence to embedded CCI bits in the content. Nakagawa later explains that the "IP" data (aka watermark or CCI bits) for copy protection are added by an encoder ("IP encoder 108"). See, ¶ 73 and ¶ 81 ("4-byte IP encoded data"). Encoding is also not generally considered equivalent or interchangeable with encryption, as encoding is principally for compression and is readable by any device with the corresponding decoding architecture, whereas encryption

is generally to restrict access to particular devices based on keys and non-reproducible algorithms and even often increases the data size.

The principle aim of the system in Nakagawa is to allow an unauthorized access device to play content back "while lowering its quality (image size, image quality, sound quality, and the like) upon playback." See, ¶ 21 – 27. Nakagawa proposes to encode a block of data and multiplex the encoded block with information used to improve the display of the data, i.e. encoding parameters, quantization data, information related to scrambling, and also authentication data. See Abs. For example, Figure 1 of Nakagawa illustrates a scheme in which quantization parameters are scrambled. See, ¶s 65-113.

Nakagawa does not encrypt secure blocks using a plurality of keys, each key being associated with a corresponding class of designation systems. Applicant notes that the Examiner appears to agree that Nakagawa does not use a plurality of keys (see O. A., pg 3), however, Nakagawa does not even appear to encrypt the data at all, let alone use different encryption for different classes of destination systems.

Nakagawa also does not appear to form a plurality of encrypted versions of secured blocks. Nakagawa appears to process each block one time, rather than creating different versions of the block. Specifically, in Nakagawa, either the block is left alone or provided with scrambled "display" information depending on the state of the "scramble ON/OFF flag." See, ¶s 76-82. There appears to be no suggestion to provide a version of the block in which is left alone and another version of the same block which has scrambled display information.

Van Rijnsoever does not cure the deficiencies of Nakagawa. Van Rijnsoever merely explains that each STB may have an associated key. See, Para. 19. Van Rijnsoever also does not appear to disclose to create multiple versions of content and does not appear to discuss a class of STBs having a common key. Further, the addition of Van Rijnsoever to Nakagawa cannot cure the fact that Nakagawa does not create multiple encrypted versions. The combination of Nakagawa and Van Rijnsoever does not meet all of the claimed limitations.

Clark also is not believed to cure the deficiencies of the above combination, and the Office action does not appear to rely on Clark for such. Furthermore, claims 3 and 10 depend from, and include all the limitations of independent claims 1 and 6. Therefore,

Applicant respectfully requests the reconsideration of dependent claims 3 and 10 and requests withdrawal of the rejection.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. Such action is earnestly solicited by the Applicant. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicant's attorney or agent at the telephone number indicated below.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Dated: February 18, 2010

Respectfully submitted,

By: /Larry T. Cullen/

Larry T. Cullen
Registration No.: 44,489

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1907